

# Re: Blocking SSH Brute-Force Attacks: What Am I Doing Wrong?

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2006-11/msg00780.html>

---

- *From:* "eculp@xxxxxxxxxxxxxxxx" <eculp@xxxxxxxxxxxxxxxx>
  - *Date:* Mon, 13 Nov 2006 08:58:48 -0600
- 

Quoting Andy Greenwood <greenwood.andy@xxxxxxxx>:

On 11/13/06, Gerard Seibert <gerard@xxxxxxxx> wrote:

On Monday November 13, 2006 at 04:10:58 (AM) Frank Staals wrote:

I had the same 'problem'. As said it's not really a problem since FreeBSD will hold just fine if you don't have any rather stupid user + pass combinations. ( test test or something like that ) Although I thought it was annoying that my intire log was clouded with those brute force attacks so I just set sshd to listen at an other port then 22. Maybe that's a acceptable solusion for you ? You can change the ssh port in /etc/ssh/sshd\_config

Security through obscurity is a bad idea. Rather, use SSH key based authentication exclusively. Turn off all of the password stuff in sshd\_config. Laugh at the poor fools trying to break in.

I second this notion. I had bruteforceblocker running and recently switched to key based auth only. The good news is no one is breaking in. the bad news is that my server is remote and difficult to get physical access to and the only key I uploaded initially was my work PC. Tried to get in from home over the weekend and found that I had locked myself out! doh! Just make sure that you have at least one PC you can get to from anywhere which has a key to get into your server.

## Re: Blocking SSH Brute-Force Attacks: What Am I Doing Wrong?

If you are using pf. A quick google search give you several differing versions of what I am using on the servers that I maintain.

<http://www.google.com.mx/search?hl=es&q=%2Bmax-src-conn-rate+%2Bpf+brute+force&btnG=B%C3%BAsqueda>

They are all max-src-conn-rate based and use the sysutils/expiretable port to clear the blocked IP's.

An example that I haven't read is here:

[http://johan.fredin.info/openbsd/block\\_ssh\\_bruteforce.html](http://johan.fredin.info/openbsd/block_ssh_bruteforce.html)

I just took one and tweaked it over time and it works great.

I only allow 3 login attempts in 30 minutes, so the brute who is trying to force his way in had better be a very good guesser;)

I did a bit of restricting in sshd\_config also but only remember MaxAuthTries,

An unexpected side effect of this is that now I get only one or two attempts a day and before there were multiple, simultaneous attempts 24 horas a day.

In my daily security report I see something like todays, everyday.

```
Nov 12 10:22:15 HOME sshd[82578]: Invalid user staff from 203.152.218.209
Nov 12 10:22:22 HOME sshd[83191]: Invalid user sales from 203.152.218.209
Nov 12 10:22:29 HOME sshd[83489]: Invalid user recruit from 203.152.218.209
Nov 12 12:47:10 HOME sshd[18369]: Invalid user staff from 24.11.169.203
Nov 12 12:47:12 HOME sshd[18421]: Invalid user sales from 24.11.169.203
Nov 12 12:47:15 HOME sshd[18425]: Invalid user recruit from 24.11.169.203
```

Before there were pages and pages. If you aren't using PF there may be something similar to max-src-conn-rate in your firewall, if not, you may want to convert ;)

Good luck,

ed

—  
Gerard

Mail from '@gmail' is rejected and/or discarded here. Don't waste your time!

---

freebsd-questions@xxxxxxxxxxxxx mailing list  
<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>  
To unsubscribe, send any mail to  
"freebsd-questions-unsubscribe@xxxxxxxxxxxxx"

Re: Blocking SSH Brute-Force Attacks: What Am I Doing Wrong?

--

I'm nerdy in the extreme and whiter than sour cream

---

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"

---

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"